Kiteworks

SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet

BRIEFING EJECUTIVO LATAM

El Punto de No Retorno

Defina Si Su Empresa Está Protegida o Expuesta
(Fecha límite: 1 de diciembre de 2026)

Camilo Silva
Director, LATAM
Kiteworks

El 1 de diciembre de 2026, todo residente chileno adquiere el derecho a preguntar qué decidió un sistema automatizado sobre él.

Y a exigir que se borren, corrijan o porten esos datos.

La nueva Agencia de Protección de Datos Personales (APDP) puede auditar sus registros de tratamiento. Imponer multas de hasta el 4% de la facturación anual global. Publicar su nombre en un Registro Nacional de Sanciones por cinco años. La Ley 21.719 convierte la protección de datos chilena en un derecho con dientes — por primera vez.

¿Puede usted?"

Fuente: Ley N° 21.719, publicada en el Diario Oficial el 13 dic 2024 — exigible el 1 dic 2026

Kiteworks

LA LÍNEA DE TIEMPO

El Camino hacia la Ley 21.719

1999
Ley 19.628
marco antiguo

Junio 2018
Derecho
constitucional (Art. 19 N°4)

Agosto 2024
Congreso aprueba
la Ley 21.719

13 dic 2024
Ley 21.719
publicada

1 dic 2026
Ley 21.719
entra en vigencia

Ocho años de debate. Veinticuatro meses para cumplir.

Si usted trata los datos personales de un solo residente chileno — incluso desde fuera de Chile — la Ley 21.719 lo alcanza. La transición de 24 meses está por cerrarse.

Fuentes: Ley N° 21.719 (Diario Oficial 13 dic 2024); Reforma constitucional Ley 21.096 (jun 2018); Ley N° 21.663 (abr 2024); Política Nacional de IA (DS N° 20 / 2021)

EL ALCANCE

Los Operadores de Importancia Vital (OIVs) También Son Responsables del Tratamiento

147

Electricidad

Generación, transmisión, distribución + CEN

29

Telecomunicaciones

Internet, móvil, fija, radio especializada

413

Servicios Digitales

SaaS, IaaS, hosting, MSPs, SOC/NOC, fintech

34

Banca y Pagos

Bancos, aseguradoras, operadores de tarjetas

114

Salud

Hospitales, mutuales, clínicas privadas

20

Empresas Estatales

ENAP, Metro, Correos, puertos, EFE

158

Órganos del Estado

Ministerios, defensa, hacienda, la propia Agencia Nacional de Ciberseguridad (ANCI)

915

OIVs definitivos

de 1,712 preliminares — Resolución Exenta N°87 17 dic 2025

Kiteworks

Lo Que la Ley 21.719 Realmente Exige

SIETE PRINCIPIOS FUNDAMENTALES

Todo tratamiento debe cumplir

1. **Licitud y lealtad :** Base legal válida, sin engaño
2. **Limitación de finalidad :** Datos solo para los fines declarados
3. **Proporcionalidad:** Adecuados, pertinentes, mínimos
4. **Calidad de los datos:** Exactos, mantenidos al día
5. **Responsabilidad:** Demostrar cumplimiento, siempre
6. **Transparencia:** Titulares claramente informados
7. **Privacidad desde el diseño :** Protección desde el diseño del proyecto

El principio de responsabilidad exige demostrar el cumplimiento — no solo cumplirlo. La evidencia documentada es el nuevo estándar.

Por qué importa para la IA: Todo principio aplica a los flujos de IA — limitación de finalidad, transparencia y privacidad desde el diseño son los más difíciles de incorporar a posteriori.

SEIS BASES LEGALES PARA EL TRATAMIENTO

Elija una antes de tratar cualquier dato

1. **Consentimiento:** Informado, específico, revocable
2. **Necesidad contractual:** Ejecutar un contrato con el titular
3. **Obligación legal:** Tratamiento exigido por otra ley
4. **Interés legítimo:** Responsable o tercero, requiere prueba de ponderación
5. **Interés vital:** Proteger la vida o la integridad física
6. **Datos sensibles:** Solo el consentimiento o excepciones legales acotadas justifican el tratamiento

Las categorías sensibles incluyen salud, biométricos, genéticos, opiniones políticas, creencias religiosas y orientación sexual — y requieren consentimiento explícito, informado y por escrito.

Fuente: Ley N° 21.719 sobre Protección de Datos Personales — Artículos 3, 12, 16

Kiteworks

La IA Está Reescribiendo el Manual de Protección de Datos

Finalidad

limitación vs. entrenamiento de IA

Datos recolectados para un fin entrenan modelos usados para muchos

Consentimiento

vs. datos inferidos

Los modelos infieren atributos sensibles a partir de entradas no sensibles

Minimización

vs. RAG y embeddings

La recuperación trae más contexto del necesario por diseño

Supresión

vs. modelos entrenados

Una vez que los datos están en los pesos del modelo, la eliminación es técnicamente incierta

Explicación

vs. opacidad

El Artículo 8 bis exige explicaciones que la IA en producción no puede entregar de forma nativa

Transferencia

vs. IA-como-servicio

Cada llamada a una API es una posible transferencia transfronteriza que la mayoría no ha evaluado

Fuentes: Ley N° 21.719 (Artículos 4, 6, 8 bis); GDPR (comparado); Kiteworks 2026 Forecast Report — el 63% de las organizaciones no puede hacer cumplir limitaciones de finalidad sobre agentes de IA

Kiteworks

La Red de Reguladores — Seis Autoridades, Un Paquete de Evidencia

APDP

Agencia de Protección de Datos Personales

Ley 21.719 — debe estar operativa para jun 2026

ANCI

Agencia Nacional de Ciberseguridad

Ley 21.663 — operativa desde ene 2025

CMF

Comisión para el Mercado Financiero

Open Finance, fintech, banca — NCG 514 vigente desde jul 2026

SUSESO

Superintendencia de Salud

Supervisión de datos de salud + derechos del paciente Ley 20.584

Tribunales

Constitucional + Suprema

Precedente Worldcoin — respaldo judicial ya operativo

+ IA

Gobernanza de IA

Según la Política Nacional de IA (DS N° 20 / 2021)

Fuentes: Ley N° 21.719 (APDP); Ley N° 21.663 (ANCI); Ley 21.521 + NCG 514 (CMF); Ley 20.584 (SUSESO); Constitución Art. 19 N°4 (Tribunales); Política Nacional de IA / DS N° 20 / 2021

FISCALIZACIÓN

Sanciones Con Dientes — y Una Forma de Suavizarlas

Del techo de USD $3,500 a multas basadas en ingresos

La Ley 19.628 imponía un techo de multas de aproximadamente USD $3,500 — insignificante para cualquier operador comercial. La Ley 21.719 construye un sistema escalonado, con escalamiento basado en ingresos para **reincidentes.**

NIVEL 1: ~USD $368K	Infracciones leves (hasta 5,000 UTM)
NIVEL 2: ~USD $725K	Infracciones graves (hasta 10,000 UTM)
NIVEL 3: ~USD $1.45M	Infracciones gravísimas (hasta 20,000 UTM)
REINCIDENCIA	2%–4% de la facturación anual — reincidencia Nivel 2/3 (no PyME)

Además: Registro Nacional de Sanciones — registro público de infractores, mantenido por 5 años. UTM = Unidad Tributaria Mensual.

MITIGACIÓN

Modelo

de Prevención de Infracciones — programa chileno voluntario certificado de cumplimiento. Tratado como factor atenuante en cualquier procedimiento sancionatorio.

Qué contiene un MPI

- Evaluación documentada de riesgos, controles y gobernanza — adoptados antes de cualquier infracción
- Designación obligatoria de DPO cuando se adopta voluntariamente un MPI
- Certificación externa — modelada sobre el marco de la Ley de Responsabilidad Penal Corporativa chilena
- El MPI es su paquete de evidencia defensiva — combinado con registros de auditoría de grado FIPS, reduce materialmente la exposición a sanciones

Un MPI no previene una infracción — cambia cómo el regulador pondera su exposición cuando ocurre una.

Kiteworks

QUÉ HACER EN LOS PRÓXIMOS 90 DÍAS

Tres Movimientos Antes del 1 de Diciembre de 2026

01

Mapee sus datos personales – y designe a su DPO

Mapee cada sistema, repositorio y SaaS donde viven los datos de los residentes chilenos — en correo electrónico, intercambio de archivos, MFT, SFTP, formularios web y APIs. Designe al DPO que asumirá las solicitudes ARCOP+, las DPIAs y la coordinación con la APDP. Impulsado por el descubrimiento y la clasificación de datos de Kiteworks en cada canal por el que se mueven datos personales.

02

Construya la capa de consentimiento y cumplimiento ARCOP+

Implemente la captura de consentimiento y la satisfacción de derechos como una capacidad en tiempo de ejecución, no como un documento de políticas. Impulsado por el Motor de Políticas de Datos de Kiteworks: aplicación ABAC en cada acceso, vinculado a la identidad de usuarios y agentes de IA, registrado a prueba de manipulación — capaz de ejecutar solicitudes ARCOP+ y explicaciones del Artículo 8 bis en los plazos regulatorios.

03

Pre-arme su paquete de evidencia para la APDP

RoPA, DPIAs para tratamientos de alto riesgo, manual de notificación de brechas y el Modelo de Prevención de Infracciones — generados continuamente, no a demanda. Impulsado por dashboards de cumplimiento de Kiteworks y plantillas predefinidas para auditorías de la APDP.

Camilo Silva · Director LATAM, Kiteworks · camilo.silva@kiteworks.com · Agende una revisión de preparación Ley 21.719 en kiteworks.com

Kiteworks

Kiteworks Genera Resultados

Gobierne la IA. Demuestre el cumplimiento. Controle sus datos.

Gobierne la IA

Cada prompt, cada agente, cada llamada API.

100% del acceso de IA registrado, atribuido y gobernado

Confianza cero controles en cada interacción de IA — la misma gobernanza que los usuarios humanos

Cumpla y Pruebe

Cada marco. Cada auditoría. Cada vez.

14+ marcos: CMMC, HIPAA, DORA, NIS 2, ISO 27001, Ley de IA de la UE

Semanas > horas de preparación de auditorías — paneles predefinidos, evidencia a demanda

Controle los Datos

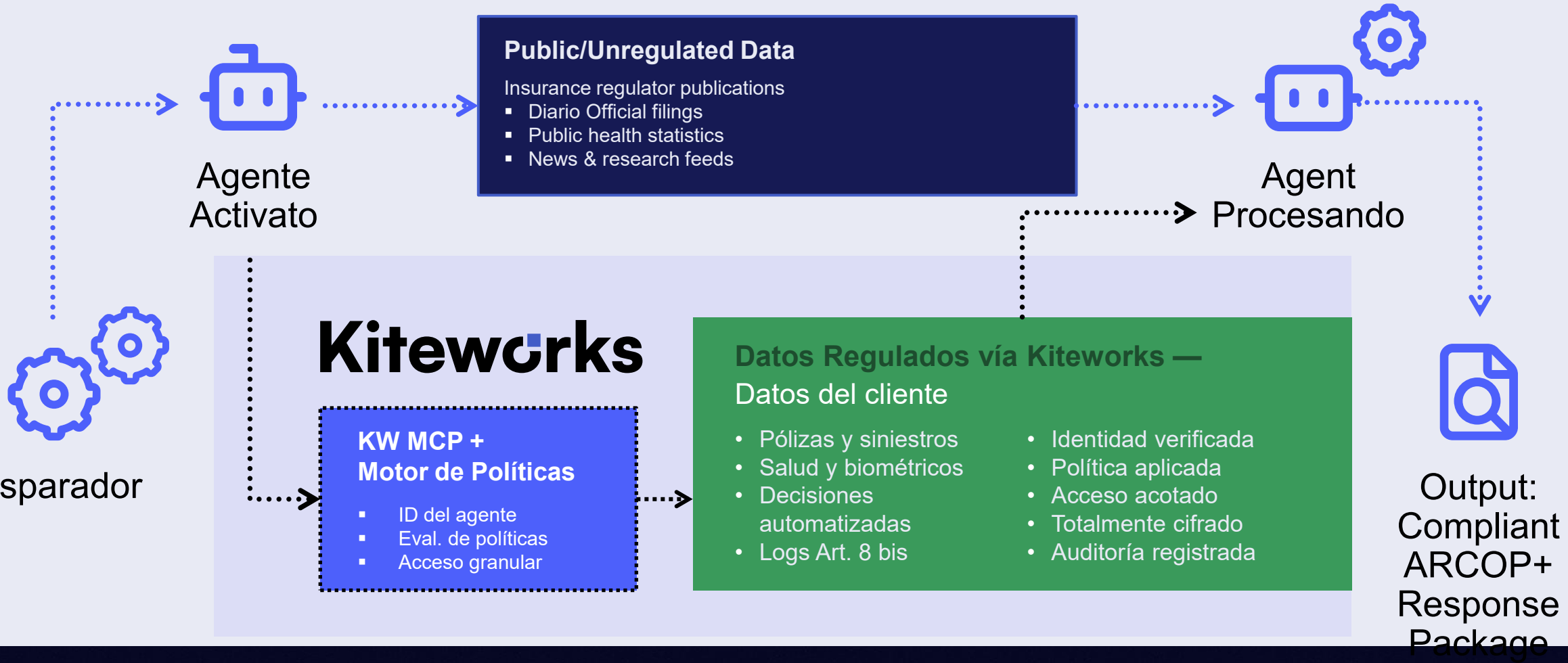
Cada canal. Cada envío. Cada registro.

7 canales, 1 plataforma correo, uso compartido de archivos, MFT, SFTP, API, formularios de datos, IA

Inquilino único + reforzado appliance virtual — seguridad integrada, no añadida

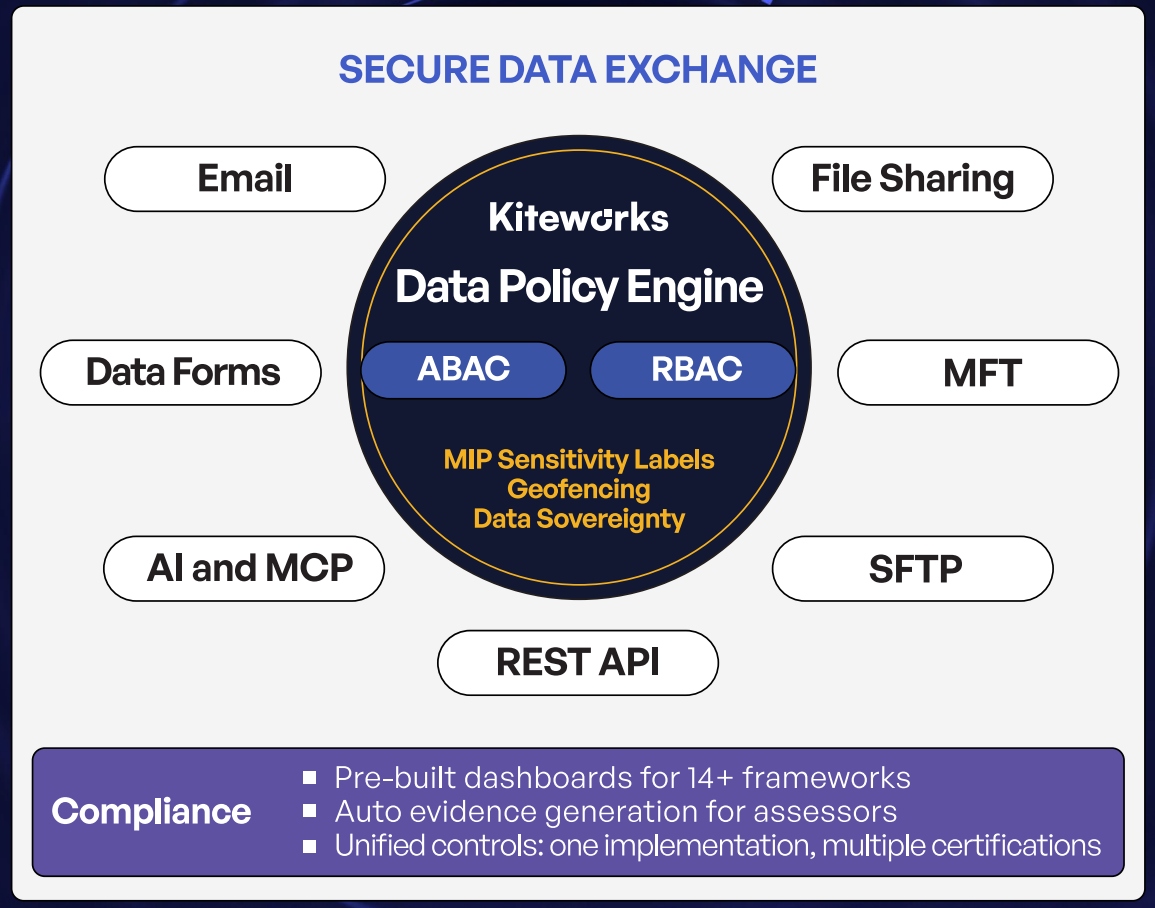
Kiteworks: Donde la IA Se Vuelve Conforme

CASO DE USO — Solicitud ARCOP+ de Derecho de Acceso — Cliente Asegurador Chileno



Kiteworks: Plano de Control para Datos Seguros

Una sola plataforma para enviar, compartir, recibir y usar datos sensibles.



CERTIFICACIONES Y VALIDACIONES

FedRAMP High en proceso

FedRAMP Moderate autorizado (2017)

FIPS 140-3 validado

SOC 2 Type II

ISO 27001 / 27017 / 27018

IRAP (Protected, Australia)

Cyber Essentials Plus

BSI C5

1999
Fundada

550+
Empleados

3,800+
Clientes Empresariales

100M
Usuarios Protegidos